

ML:JRS
F.#2019R01078

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
ONE BLACK APPLE IPHONE MODEL
A1778 SEIZED FROM BRANDON
LOMAX ON AUGUST 5, 2019,
CURRENTLY IN THE EASTERN
DISTRICT OF NEW YORK

TO BE FILED UNDER SEAL

Case No. 19-MJ-784

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, MEGAN QUINN, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property — an Apple iPhone Model A1778 — which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”) and have been since 2005. I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been personally involved in numerous investigations involving robberies. I have also received training on the uses and capabilities of cellular devices.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is one black Apple iPhone Model A1778 seized from BRANDON LOMAX on August 5, 2019 (the “Device”). The Device is currently in the custody of the ATF in the Eastern District of New York.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. Based on the facts below and my training and experience, I believe that there is probable cause to search the Device for evidence of violations of 18 U.S.C. §§ 1951(a) (Hobbs Act robbery) and 924(c) (use of a firearm during a crime of violence) by BRANDON LOMAX and others.

7. Plenty of Fish is an online dating app that is used across the United States and that is owned by a Canadian company. Plenty of Fish allows users to post photographs and profiles and to communicate through the app with other users.

8. On or about July 8, 2019, an individual (“Victim-1”) corresponded through Plenty of Fish with an individual using the name “StarBabyyy.” “StarBabyyy” purported to be a 24 year old woman in Brooklyn, New York. StarBabyyy told Victim-1 that her phone number was 347-925-6947 (the “Phone Number”). Victim-1 began texting with that number and agreed to come meet StarBabyyy at 1636 Park Place, Brooklyn, New York.

9. When Victim-1 arrived at 1636 Park Place, StarBabyyy texted him a code for the front door, which he used to enter the building. StarBabyyy then texted Victim-1 to tell him to come to the third floor, which he did.

10. When Victim-1 arrived on the third floor, he texted StarBabyy to let her know that he had arrived. She responded by text that she would be right out. But, instead, two men wearing stockings over their heads came up the stairs and accosted Victim-1 at gunpoint. The two men robbed Victim-1 of two cell phones, currency and his black Gucci sneakers before fleeing back down the stairs.

11. On or about July 10, 2019, a second individual ("Victim-2") similarly corresponded with StarBabyyy through Plenty of Fish. He too was given the Phone Number as StarBabyyy's phone number. Victim-2 texted with the Phone Number and was instructed to come to 1640 Sterling Place, Brooklyn, New York to meet StarBabyyy.

12. When Victim-2 arrived at 1640 Sterling Place, he was accosted by two men brandishing a firearm. One of the men was wearing a gray shirt, black Nike Air Force sneakers and a green bandanna on his face. The other man was wearing a white t-shirt and also had his face covered. The men took Victim-2's phone, currency and mustard yellow Air Jordan sneakers, which they placed in a small black plastic bag. The men then fled the building.

13. NYPD detectives obtained surveillance video from a building near 1640 Sterling Place. That video showed two men running away from 1640 Sterling Place on July 10, 2019. One of the men is wearing a gray shirt, black Nike sneakers and is holding a green bandanna in his hand. The video shows this man walking with his hand in his waistband in a manner that, based on my training and experience, is consistent with a person concealing a

firearm. The other man on the video is wearing a white t-shirt and a mask. The second man is also shown carrying a plastic bag containing what appears to be yellow sneakers.

Man Holding Green Bandanna



Man Wearing Mask



14. NYPD officers who have met and interacted with BRANDON LOMAX in person have reviewed images from that video and have stated that the man holding the green bandanna appears to be BRANDON LOMAX. I have also compared images from the video

to a photograph of BRANDON LOMAX and based on my comparison, I believe that the man shown in the video is BRANDON LOMAX.

15. Law enforcement obtained records from T-Mobile US, Inc. for the Phone Number. According to those records, Victim-1 was in contact with the Phone Number on July 8, and Victim-2 was in contact with the Phone Number on July 10.

16. According to subscriber records for the Phone Number, the Integrated Circuit Card Identifier ("ICCID") for the SIM card associated with the Phone Number is 8901260185747250202.

17. On August 5, 2019, BRANDON LOMAX was arrested by the NYPD in Brooklyn, New York, after being found in possession of a firearm. At the time of his arrest, LOMAX was found to be in possession of the Device, a black Apple iPhone model A1778. The SIM card contained in the Device bore ICCID 8901260185747250202, i.e., the same ICCID associated with the Phone Number.

18. Based on these facts, as well as my training and experience, I believe that there is probable cause to believe BRANDON LOMAX used the Device and Plenty of Fish to lure Victim-1 and Victim-2 to be robbed.

19. I further believe that the Device likely contains evidence of LOMAX's use of Plenty of Fish and LOMAX's communications with victims, as well as other evidence.

20. For example, I know that criminals frequently use telephones such as the Device to communicate about criminal conduct and to store photographs, videos, and other records that would be evidence of criminal conduct. In particular, those who are committing robberies often use telephones to communicate with co-conspirators. As discussed below, I also know that telephones such as the Device frequently track their users locations, which

could provide evidence of LOMAX's and any co-conspirators' locations on the day of the robberies and during any subsequent meetings.

21. The Device is currently in the lawful possession of the ATF. After the Device was seized from LOMAX incident to arrest on August 5, 2019, the NYPD subsequently provided it to the ATF.

22. The Device is currently in the custody of the ATF in the Eastern District of New York. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as it was when the Device first came into the possession of law enforcement.

TECHNICAL TERMS

23. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video;

storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same

capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

24. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA and to access the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

25. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is

probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

28. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

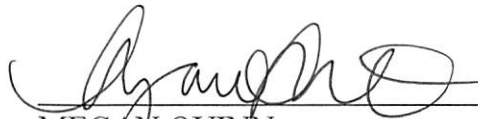
29. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

30. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation as not all of the targets of this investigation will be searched at this time. Premature disclosure of the contents of this affidavit and

related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Megan Quinn', is written over a horizontal line.

MEGAN QUINN

Special Agent, Bureau of Alcohol, Tobacco,
Firearms and Explosives

Sworn to before me this
5th day of September, 2019

/s/ RLM

THE HONORABLE ROANNE L. MANN
CHIEF UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is one black Apple iPhone Model A1778 seized from BRANDON LOMAX on August 5, 2019 (the “Device”). The Device is currently in the custody of the ATF in the Eastern District of New York.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, Sections 924(c) and 1951(a), and involve BRANDON LOMAX and any co-conspirators since July 1, 2019, including:

- a. any evidence relating to the use of Plenty of Fish or other dating apps;
- b. communications regarding robberies, firearms or stolen goods;
- c. any internet or search history relating to robberies, firearms or stolen goods;
- d. photographs, videos, notes or sound recordings relating to robberies, firearms or stolen goods;
- e. any information regarding communications software used by BRANDON LOMAX and his co-conspirators;
- f. any information recording BRANDON LOMAX's or his co-conspirator's schedule, location or travel from July 1, 2019 to August 5, 2019;
- g. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the law enforcement agents may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.